SIEMENS
Ingenuity for life

Cyber Security for Industries

Dr. Rainer Falk
Principal Key Expert

SIEMENS
Ingenuity for life

Werner von Siemens: At a glance

1816 – 1892

Werner von Siemens was a responsible entrepreneur and far-sighted inventor whose name soon became a household word around the world. Far ahead of his time, he recognized and fostered the link between science and technology.

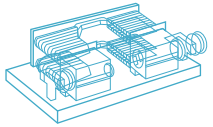
“In my youth, I dreamed of founding an enterprise of world standing comparable to that of the Fugger dynasty …”

Werner von Siemens, 1887

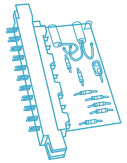
Milestones of a 170-year history

1816 – 1892
Company founder, visionary and inventor

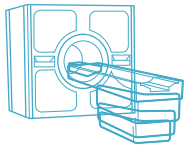
Werner von Siemens



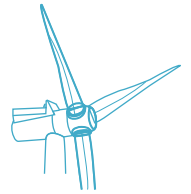
1866
The dynamo makes electricity part of everyday life



1959
SIMATIC makes Siemens a leader in automation technology



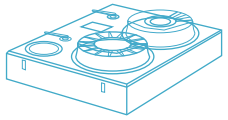
1983
First magnetic resonance imaging scanner goes into operation



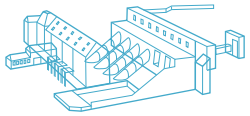
2012
Test operation of the world's largest rotor for offshore wind turbines

Siemens innovations over the past 170 years

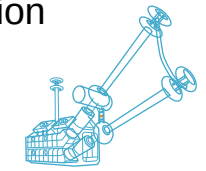
1847
Pointer telegraph lays the foundation of Siemens as a global company



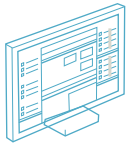
1925
Siemens electrifies the Irish Free State with a hydroelectric power plant.



1975
Breakthrough of high-voltage direct-current (HVDC) transmission



2010
TIA Portal takes automation a stage further



2015
Sinalytics puts digital services for industry on a new footing

Vision 2020 –
A consistent company concept

E-A-D – a complete system

With our positioning along the **electrification** value chain, we have know-how that extends from power generation to power transmission, from power distribution and smart grids to the efficient application of electrical energy.

With our outstanding strengths in **automation**, we're well equipped for the future and the age of **digitalization**.

Digitalization at Siemens – Productivity lever for our customers

SIEMENS
Ingenuity for life

- Cooperation and mobile IT
- Smart data and analytics
- Cloud technologies
- Connectivity and Web of Systems
- Cyber security

Improved productivity, shorter time-to-market

Greater flexibility and stability

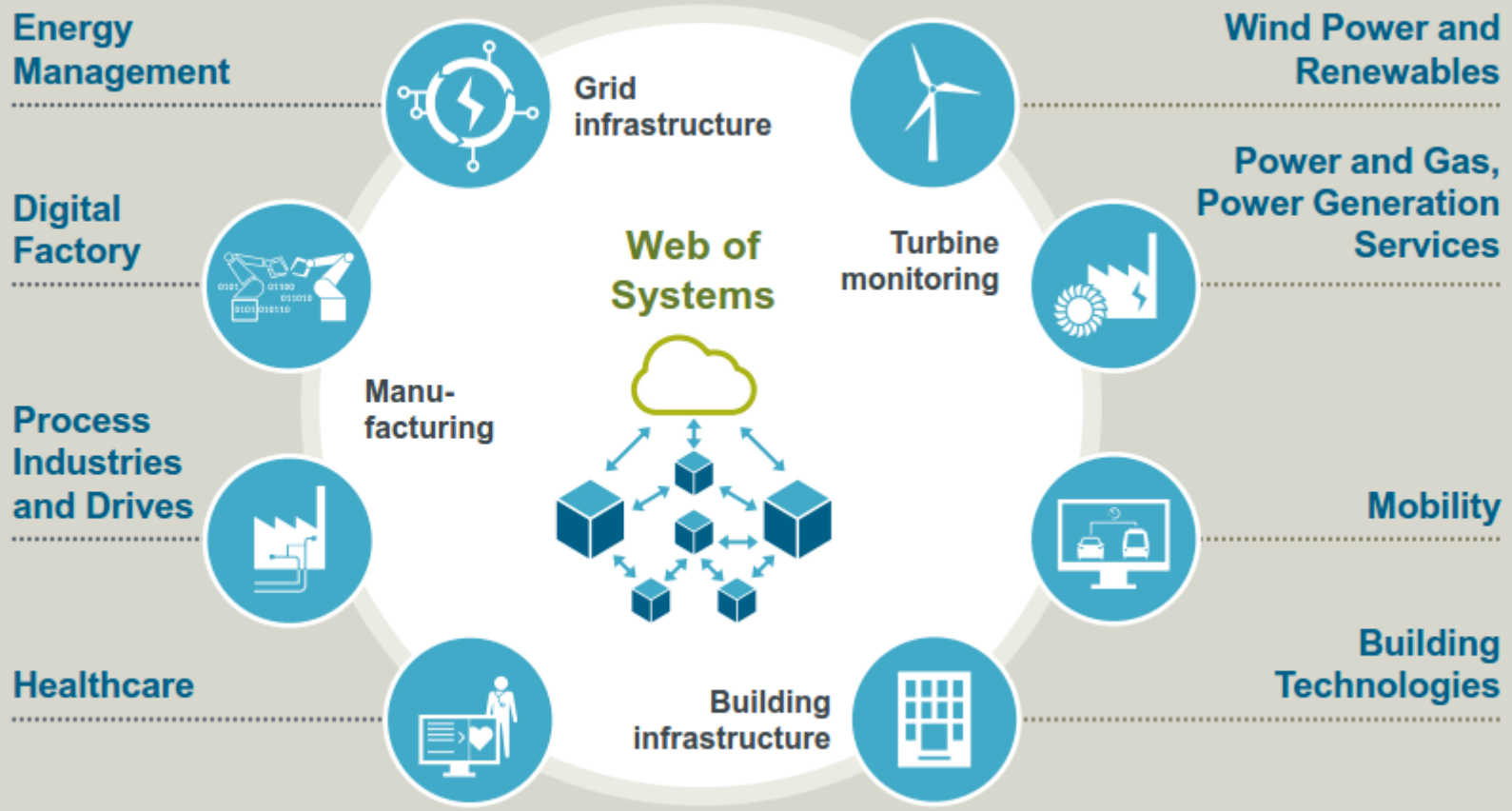
Higher availability and efficiency

Design and engineering → **Automation and operation** → **Maintenance and services**

Linking the virtual and real worlds along the entire value chain of customers

	Vertical software	Digital services
Revenue, FY 2015	€3.1 billion	€0.6 billion
Profitability	++	+++
Market growth	+9%	+15%

Concept for the Industrial Application of the Internet of Things – The Web of Systems provides security for critical infrastructure



- Siemens believes the Internet of Things has tremendous potential
- In critical infrastructure, customers have much higher requirements regarding reliability, service life and data protection
- For this reason, in a Web of Systems the data is processed locally
- This ensures that the knowledge and the intellectual property of our customers remain protected
- Siemens is already using this technology in many projects today

Our innovative power in figures – Siemens as a whole and Corporate Technology

Expenditures for research and development

€4.5 billion
Expenditures for R&D in fiscal 2015

32,100
R&D employees[1]

Inventions and patents – securing our future

7,650
inventions[1]

3,700
patent applications

University cooperations – our knowledge edge

9
CKI universities[2]

16
principal partner universities

1 In fiscal 2015 **2** Centers of Knowledge Interchange

Corporate Technology – our competence center for innovation and business excellence[3]

7,800
employees worldwide

5,300
software developers

1,600
researchers

400
patent experts

3 Employee figures: Status September 30, 2015

Our organization – Corporate Technology at a glance

SIEMENS
Ingenuity for life

Corporate Technology (CT)
CTO – Prof. Dr. Siegfried Russwurm

Business Excellence, Quality Management, *top*+
- Business excellence
- Quality management
- Internal process and production consulting

Corporate Intellectual Property
- Protection, use and defense of intellectual property
- Patent and brand protection law

Development and Digital Platforms
- Competence center for horizontal and vertical product-and-system integration as well as software, firmware, and hardware engineering

Innovative Ventures
- Access to external innovations
- Start-up foundation
- Commercialization of innovations

Research in Digitalization and Automation
- Research activities covering all relevant areas in digitalization and automation for Siemens

Research in Energy and Electronics
- Research activities relating to energy and electrification, electronic, new materials and innovative manufacturing methods

Technology and Innovation Management
- Siemens' technology and innovation agenda
- Standardization, positioning regarding research policy
- Provision of publications relating to R&D

University Relations
- Global access to the academic world
- Top positioning in terms of university cooperations

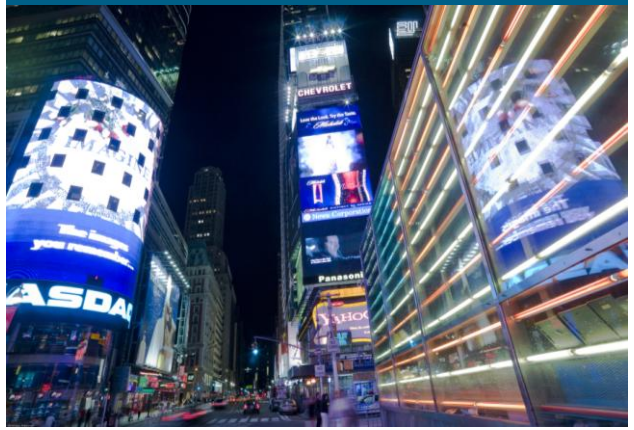
Increasing intelligence and open communication drive security requirements in various industrial environments

SIEMENS
Ingenuity for life

Process Automation

Factory Automation

Urban Infrastructures



Building Automation

Energy Automation

Mobility Systems

Our industrial society confesses a growing demand for IT-Security

IT Security trends are determined by drivers such as

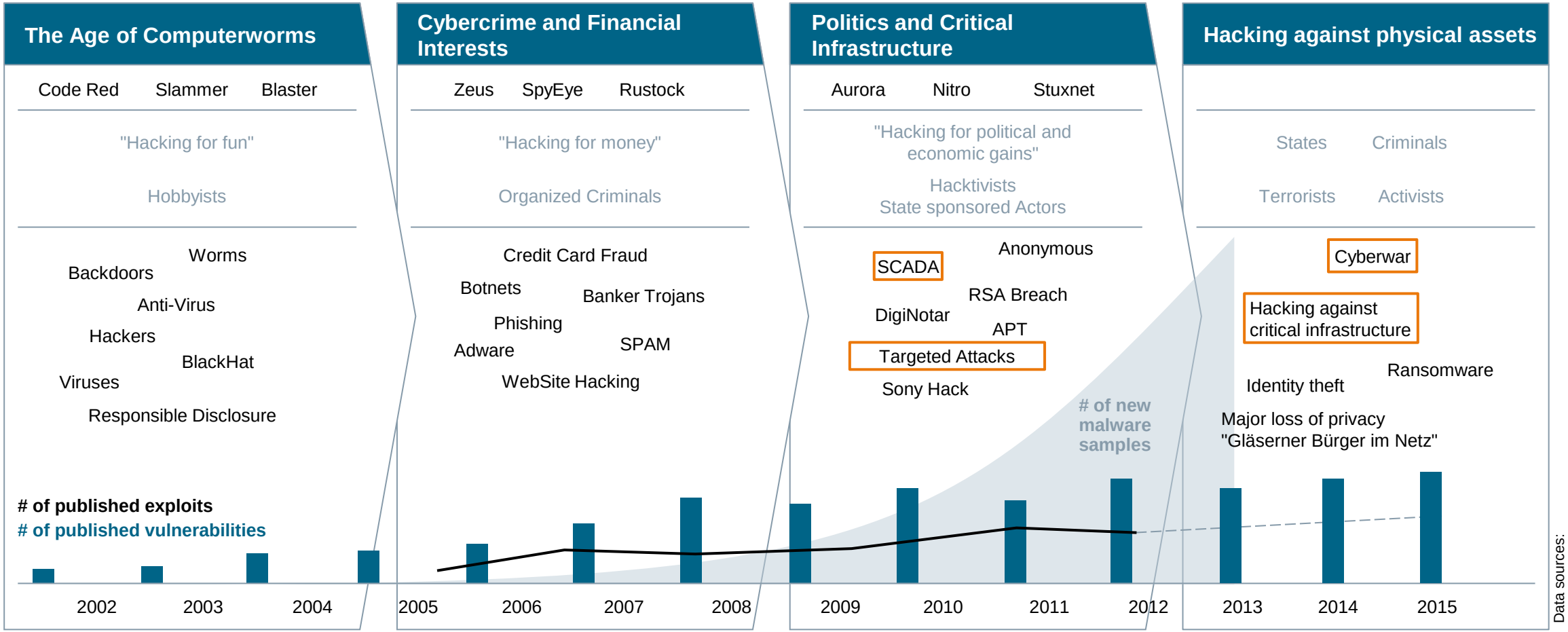
- Industry infrastructures changes (Digitalization)
- More networked embedded systems
- Increasing device-to-device communication
- Need to manage intellectual property

And

- Increasing international organized crime
- Privacy
- Compliance enforcement
- Cyber war fare
- Cloud/Virtualization
- PDAs, Smart Mobiles
- Social Networks / data mining concepts
- ….

The threat level is rising – Attackers are targeting critical infrastructures

Evolution of attacker motives, vulnerabilities and exploits



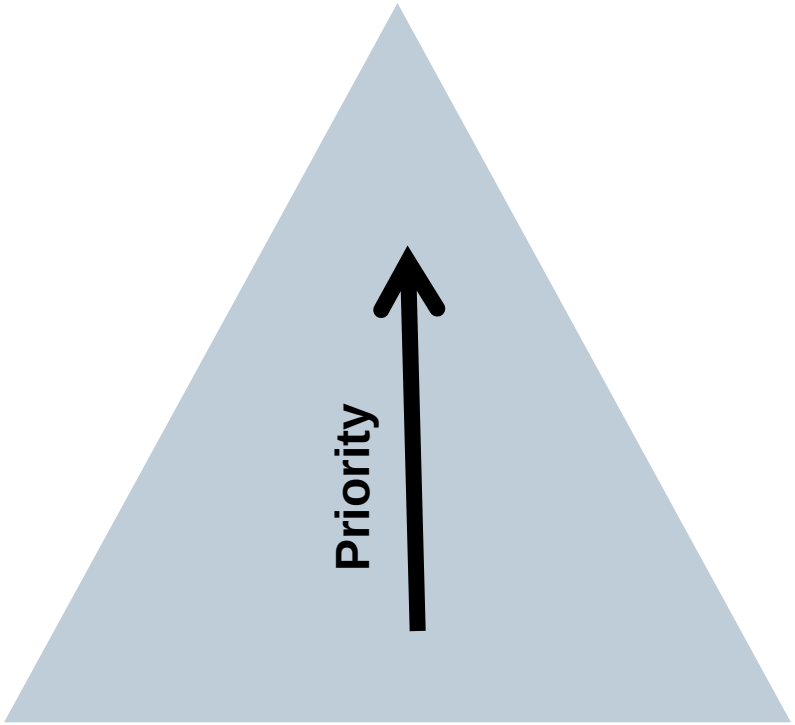
Industrial systems and office world have different management & operational characteristics

	Industrial Systems 	Office IT 
Protection target for security	Production resources, incl. logistics	IT- Infrastructure
Component Lifetime	Up to 20 years	3-5 years
Availability requirement	Very high	Medium, delays accepted
Real time requirement	Can be critical	Delays accepted
Physical Security	Very much varying	High (for IT Service Centers)
Application of patches	Slow / restricted by regulation	Regular / scheduled
Anti-virus	Uncommon, hard to deploy, white listing	Common / widely used
Security testing / audit	Increasing	Scheduled and mandated

The CIA pyramid is turned upside down in industrial automation and control systems

SIEMENS
Ingenuity for life

Industrial Automation and Control Systems	Office IT Systems
Availability	**Confidentiality**
Integrity	**Integrity**
Confidentiality	**Availability**



Industrial systems and office world have different functional security requirements

	Industrial Systems	Office IT
Security Awareness	Increasing	High
Security Standards	Under development, regulation	Existing
Confidentiality (Data)	Low – medium for production floor High for business-relevant know-how	High
Integrity (Data)	High	Medium
Availability / Reliability (System)	24 x 365 x …	Medium, delays accepted
Non-Repudiation	Medium to High	Medium

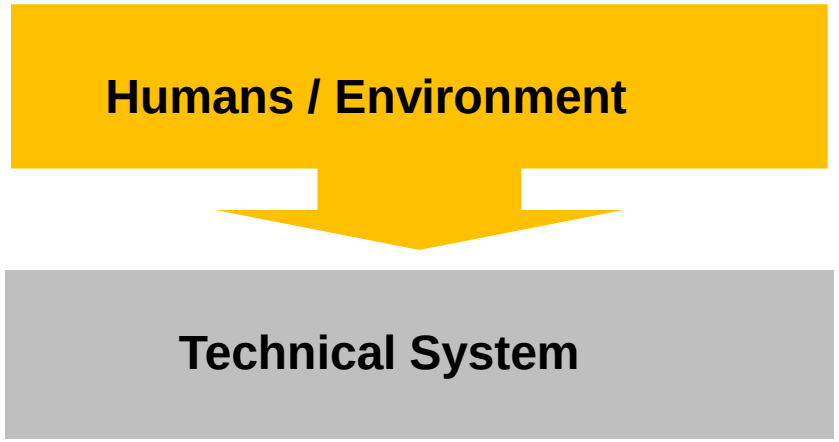
“Office“ security concepts and solutions are not directly applicable for industrial control systems

Security-by-Design is different from Safety-by-Design

SIEMENS
Ingenuity for life

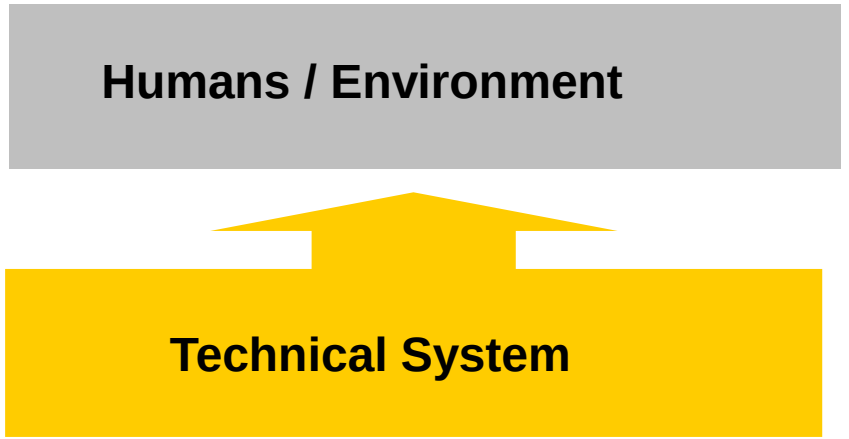
IT Security

Prevention of consequences
of threats to a system (intentionally) caused by
humans and/or environment



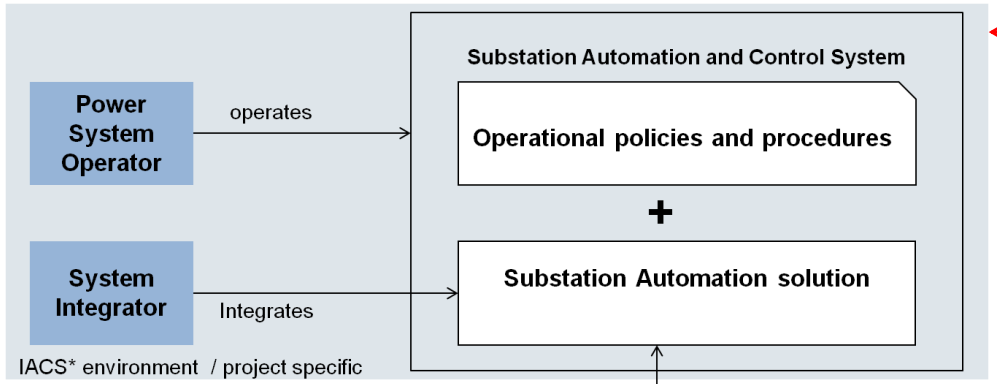
Safety

Prevention of threats to humans and
environment caused by technical systems

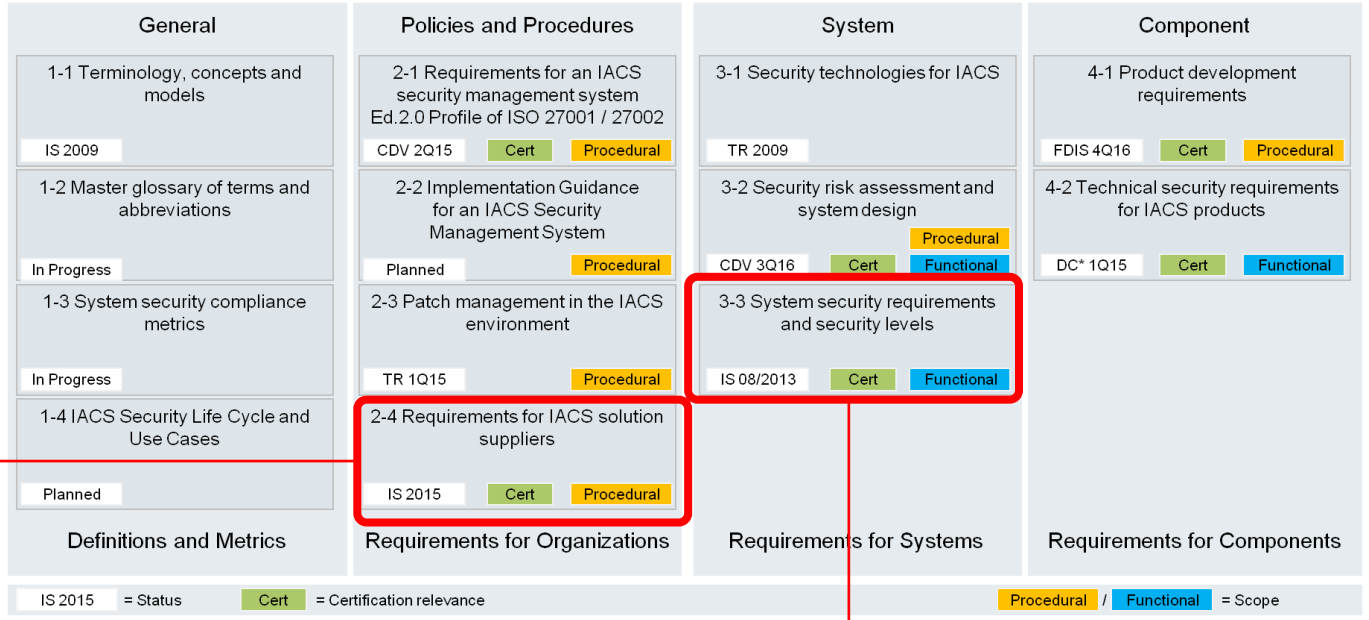


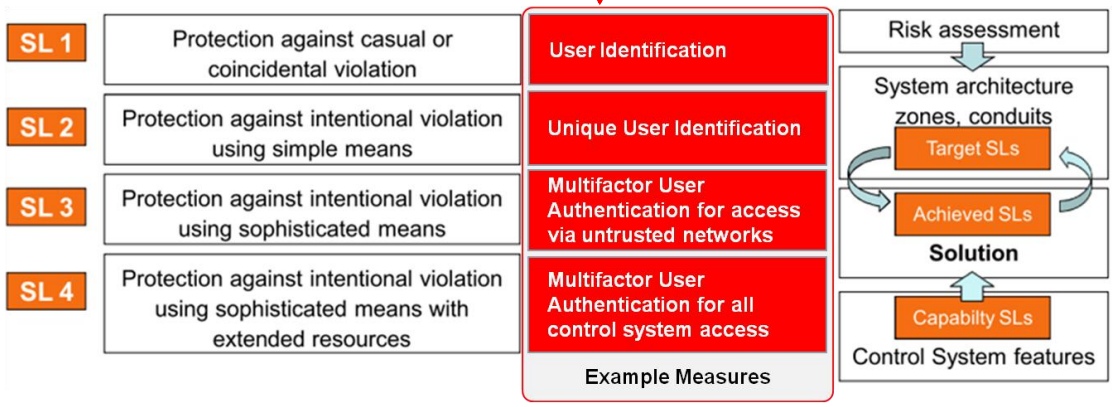
IEC62443 as standard for industrial security enables a graded security approach to achieve appropriate protection

- IEC 62443 is a framework specifying security requirements for industrial automation control systems (IACS)
- Addresses organizational and technical requirements
- Supports purpose fit security solutions by supporting security features with different strength

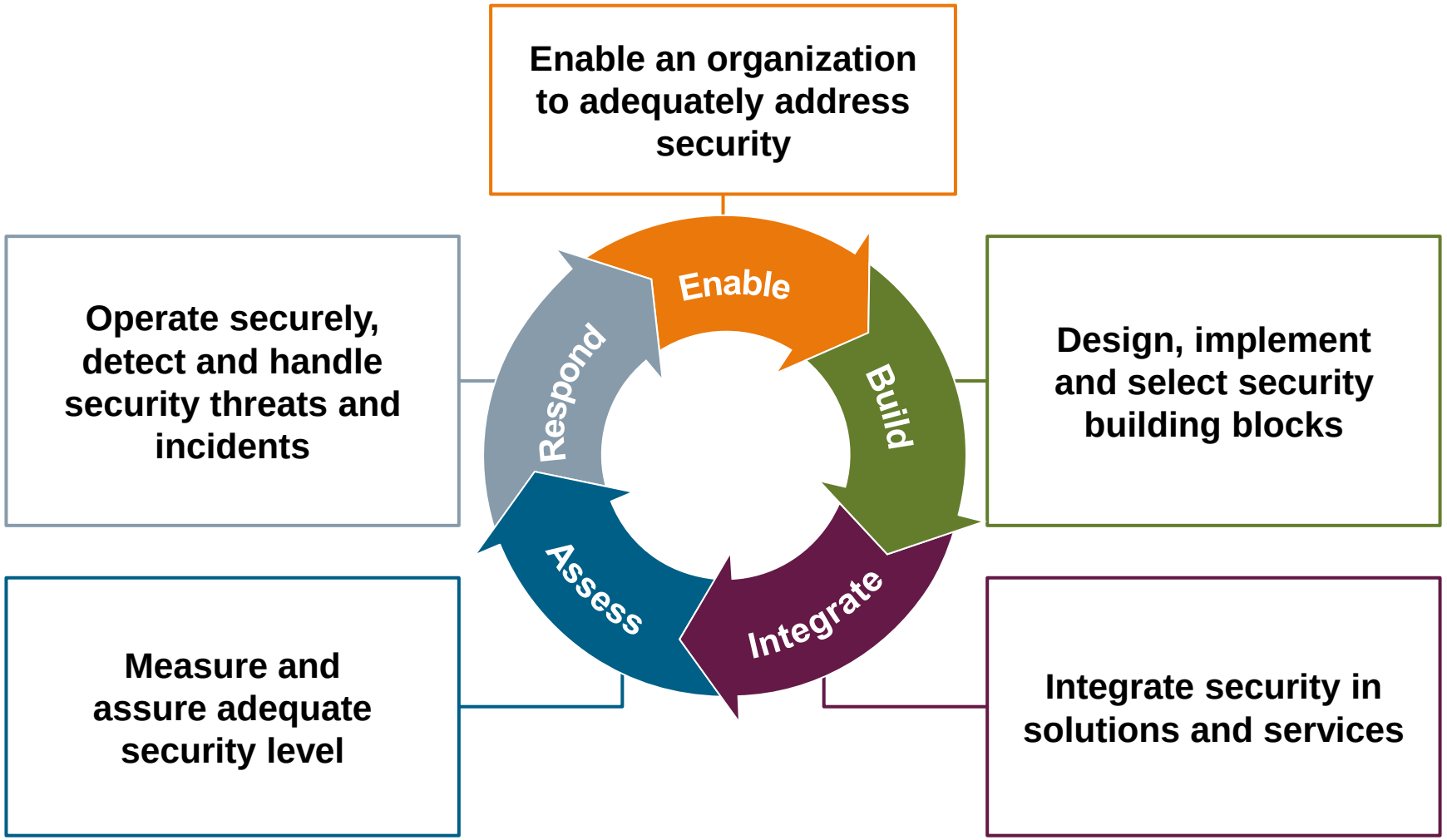


*IACS = Industrial Automation Control System





Security-by-design cares for the entire product and system life cycle



Security within Industry 4.0:
Security by design & security by default

SIEMENS
Ingenuity for life

More integrated security within applications
- …rather than just within the network (layers)
- Application based end-to-end security must be possible

Adaptive security architectures
- Agile security profiles have to be adaptable in a dynamic way.
- Fast configuration must include security.

Security for the digital model
- Security for the physical instance, its digital twin and their interactions must take place in a concerted way.

Prevention and reaction are still needed
- Security will remain moving target. There will be no final I4.0 security solution without a need for further measures.

The Future of Industry:
Security for Industry 4.0 – (some) constraints and requirements

SIEMENS
Ingenuity for life

Authentication and Secure Identities for Devices

Unforgeable identities and trust anchors are needed.
Keys respectively security credentials must be bound to the device.

B2B vs. B2C communication

Individual and short-term consideration of customer requests
(“batch-size 1”) need enhanced security

IT Security as enabler of business models

Digitalization of business processes often mandate additional measures regarding IT security. Ease-of-use and plug&operate are important pre-requisites for the acceptance of security measures.

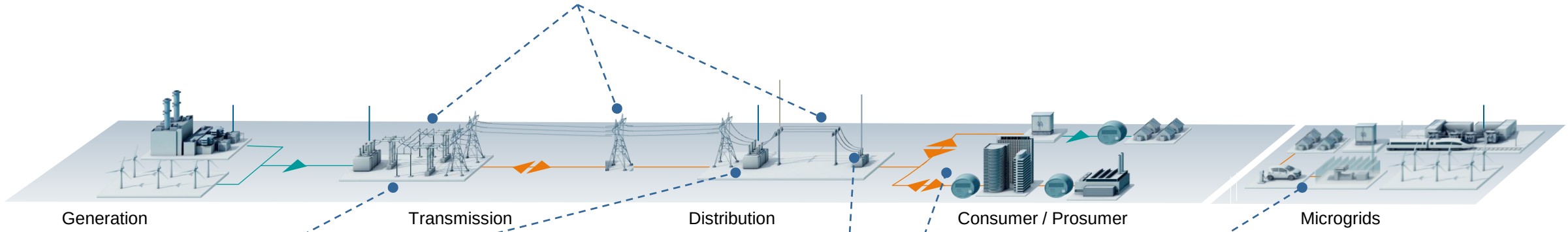
Standardization enables secure infrastructures

Security requires standardized specifications of interfaces and protocols to support requirements and to negotiate and operate security profiles (security semantics) between different domains.

Example: Smart Grid
Secure Communication supports reliable operation

SIEMENS
Ingenuity for life

2
- Power Quality Monitoring and Eventing (Transmission/Distribution, Substation)
- Communication Standards used: IEC 61850 (GOOSE)
- Security uses group- based security integrated in GOOSE (IEC 62351-6)



1
- Substation Automation (Telecontrol and Monitoring)
- Inter Control Center Communication
- Communication Standards used: IEC 60870-5-104, IEC 61850
- Remote Service
- Transport level security through TLS (IEC 62351-3/4/5)
- Application level security through X.509 based authentication + integrity. (IEC 62351-4)

3
- DER Integration (Metering & Control)
- Communication Standards used: IEC 61850, XMPP (future use)
- Transport level security through TLS (IEC 62351-3/4/5)

4
- Connecting electric vehicles to the charging infrastructure
- Communication Standards used: ISO/IEC 15118, IEC 61850
- Transport level security: TLS
- Application level security: XML Dig.Sig.

Example IEC 15118: eCar charging security
Securely connecting the vehicle to the smart grid

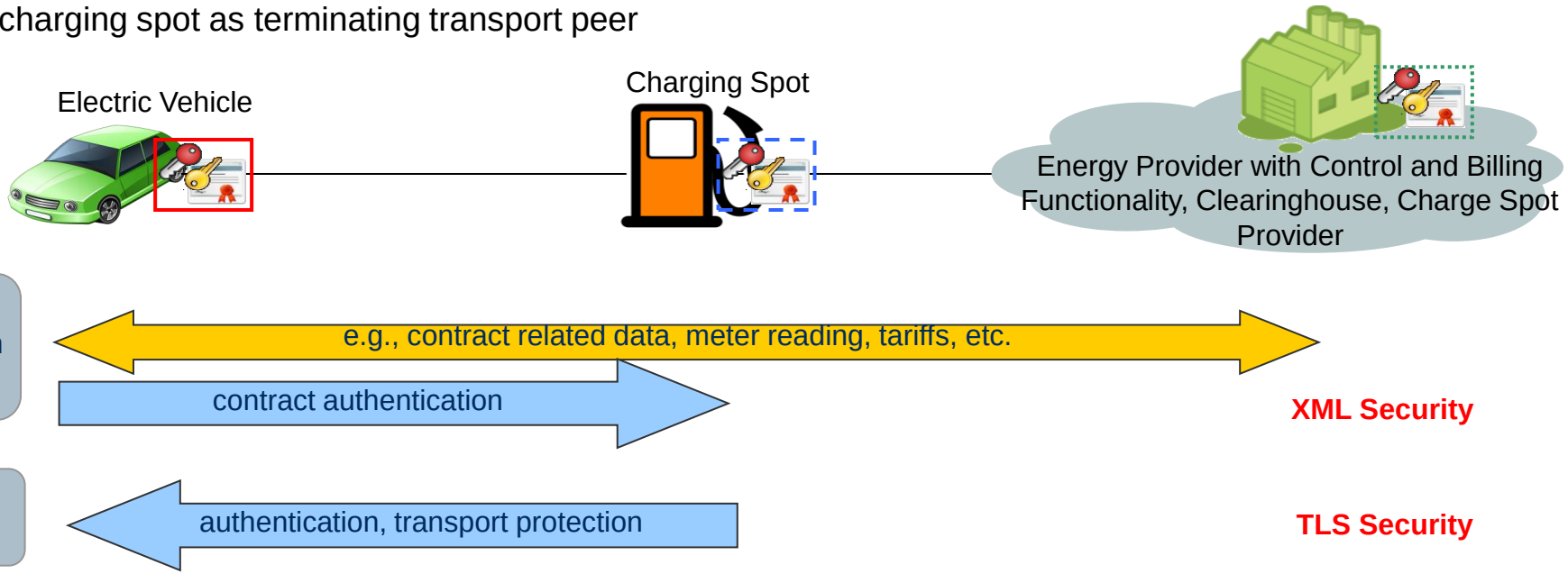
SIEMENS
Ingenuity for life

Standard for the interface between vehicle and charging station supporting

- Connection of vehicles to the power grid
- Billing of consumed energy (charging)
- Roaming of electric vehicles between different charging spot
- Value added services (e.g., software updates)

Trust Relations from the electric vehicle

- Towards backend (energy provider) for signed meter readings and encrypted information (e.g., tariff)
- Towards charging spot as terminating transport peer



IEC 15118 – Approach based on certificates and corresponding private keys (PKI)

Approach

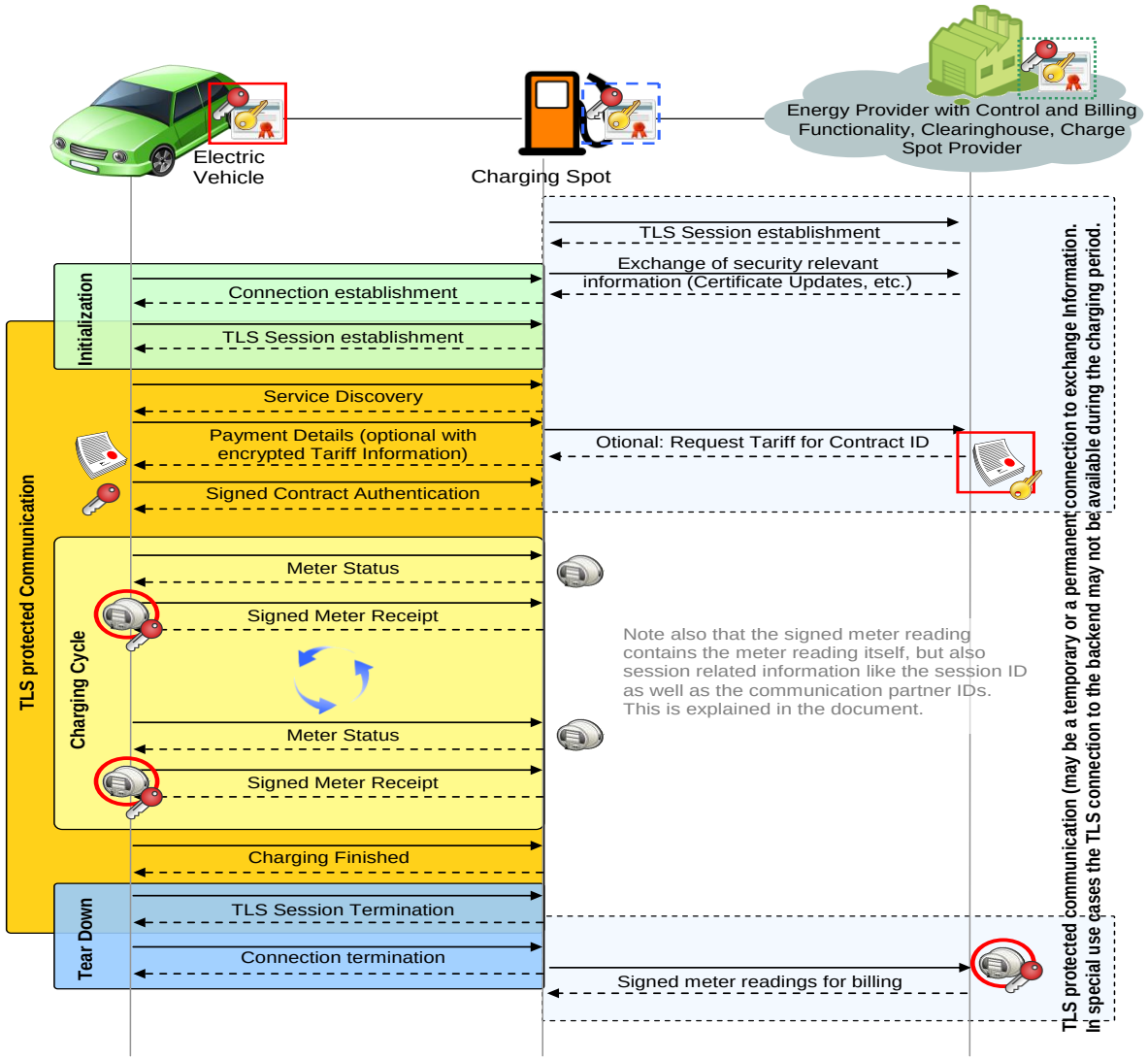
- Transport Layer Security to protect exchange between vehicle and EVSE
- Application layer security using XML security for data exchange with the backend

Credentials

- Public/private key pair incl. certificate

Connectivity

- Online and Semi-online to the backend
- Persistent connection between vehicle and EVSE during charging to exchange charging process relevant information, especially a cyclic exchange of metering data for provided energy

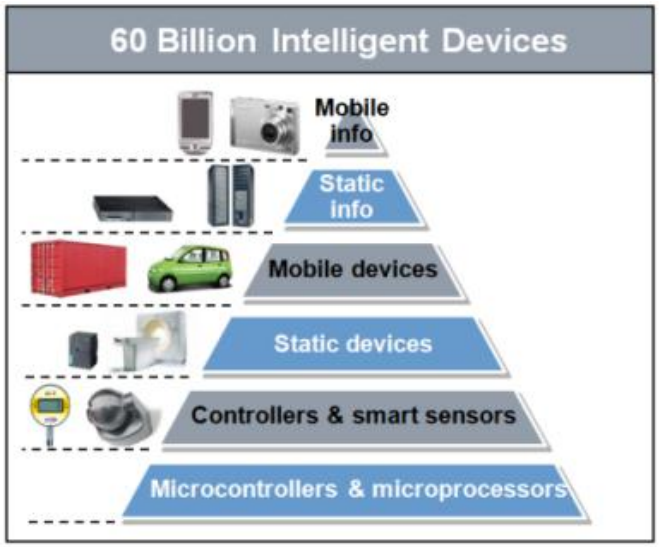


Different factors are driving the demand for IT Security

New Functionality and Architectures

Examples

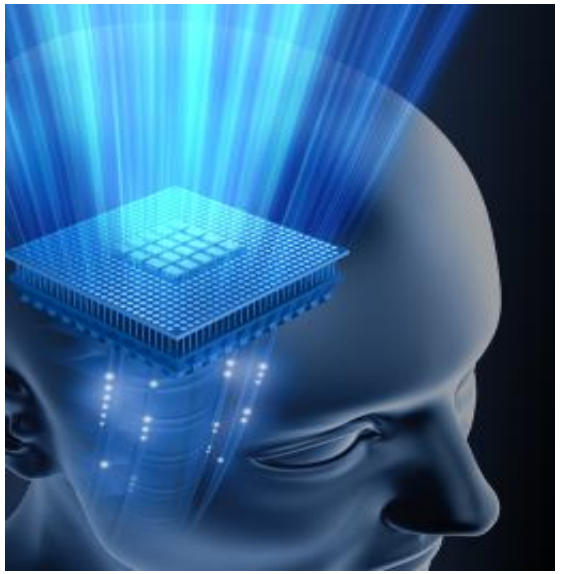
- Connectivity of devices and systems to public networks
- IP to the field
- Use of mobile devices



Security Use Case

Examples

- Know-how protection
- Licensing



Quality of Security

Examples

- Robust
- Easy to use
- Long term security

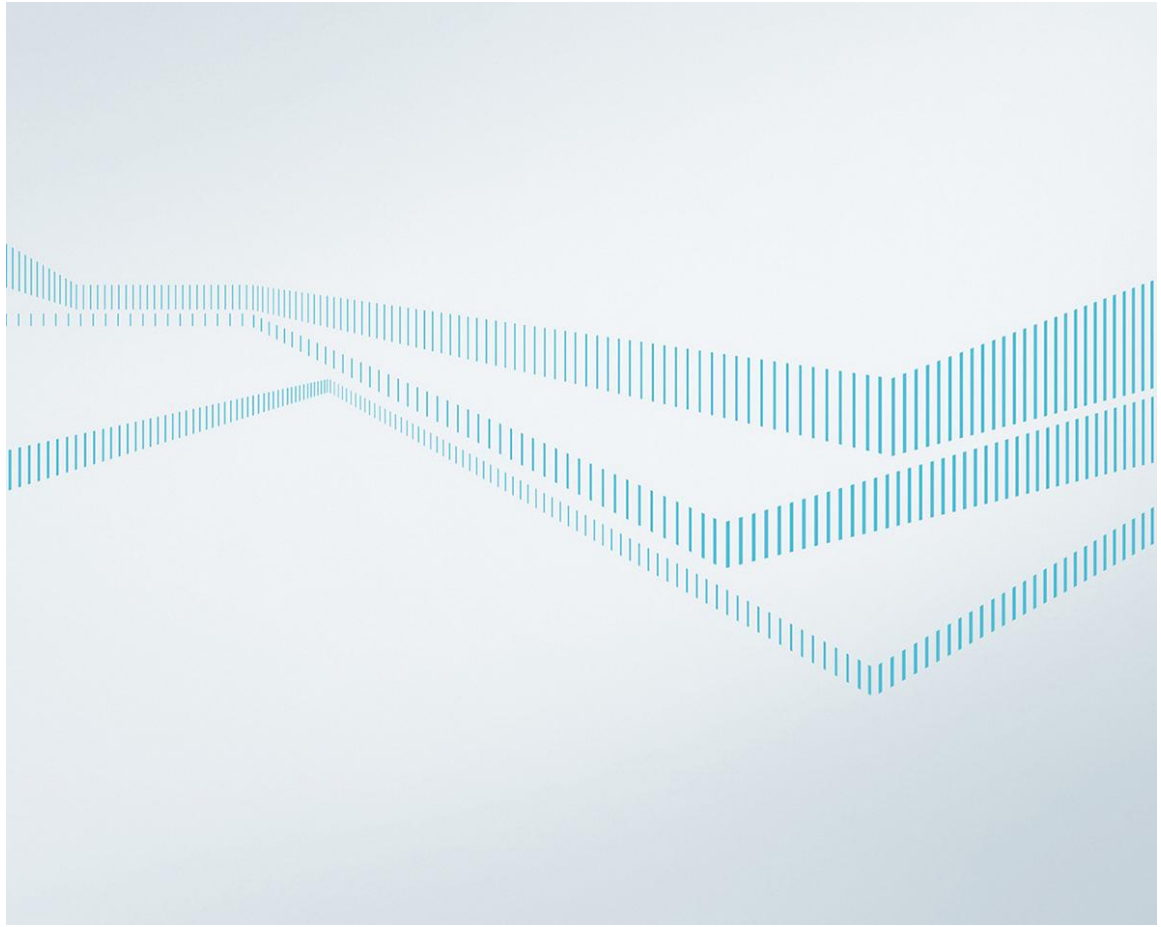
Security has to be suitable for the addressed environment

Awareness and Acceptance

Since security is not just a technical solution, which can be incorporated transparently, we need to consider how humans can get along with this issue.

This needs, especially for automation environments, actions for:

- awareness trainings
- help people to understand security measures and processes
- provide user friendly interfaces and processes



Dr. Rainer Falk
Principal Key Expert

Siemens AG
Corporate Technology
CT RDA ITS
Otto-Hahn-Ring 6
D-81739 Munich
Germany

E-mail
rainer.falk@siemens.com

Internet
siemens.com/corporate-technology

Vision 2020 –
A consistent company concept

E-A-D – a complete system

With our positioning along the **electrification** value chain, we have know-how that extends from power generation to power transmission, from power distribution and smart grids to the efficient application of electrical energy.

With our outstanding strengths in **automation**, we're well equipped for the future and the age of **digitalization**.

Digitalization at Siemens – Productivity lever for our customers

SIEMENS
Ingenuity for life

- Cooperation and mobile IT
- Smart data and analytics
- Cloud technologies
- Connectivity and Web of Systems
- Cyber security

Improved productivity, shorter time-to-market

Greater flexibility and stability

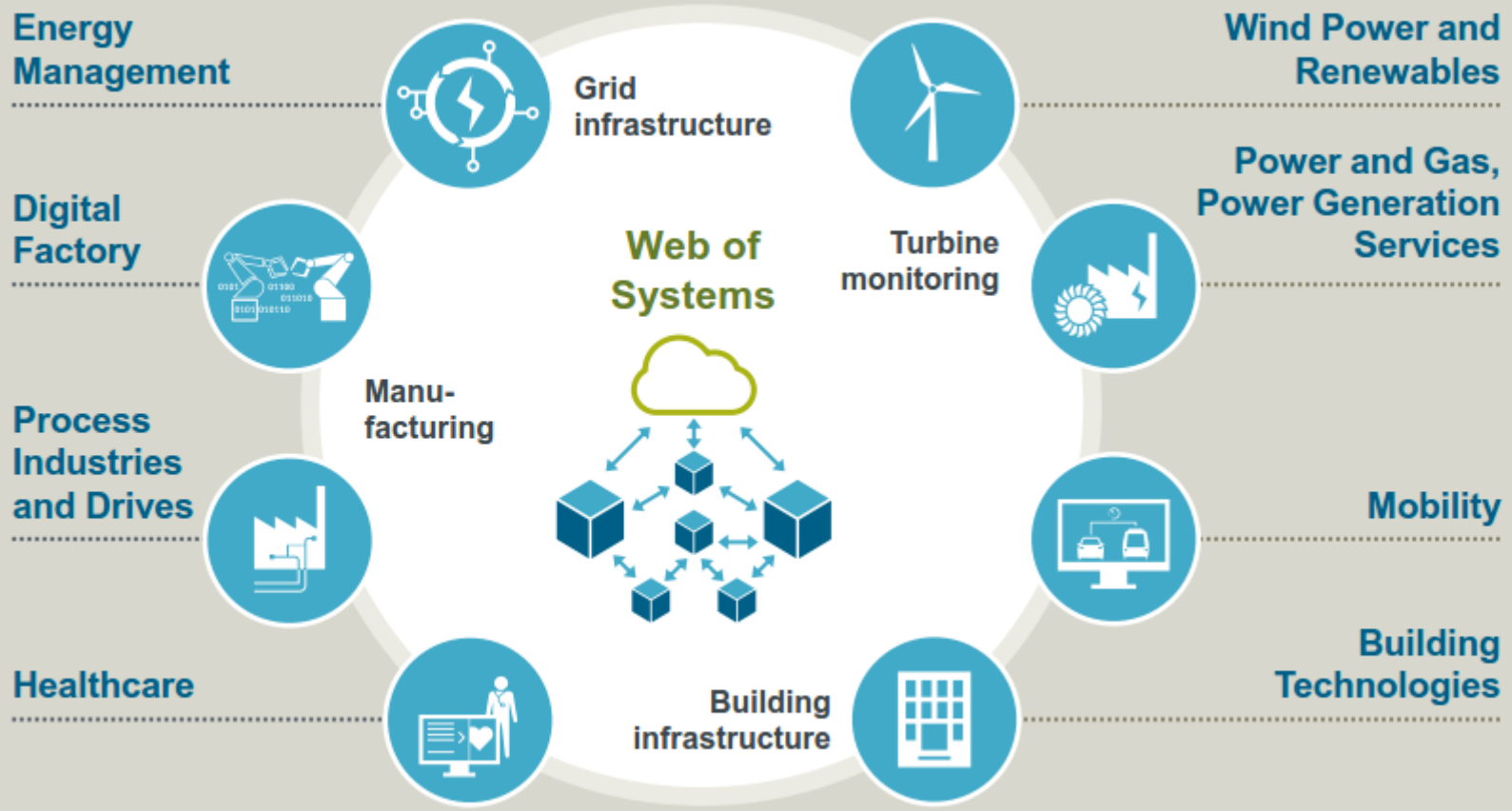
Higher availability and efficiency

Design and engineering → **Automation and operation** → **Maintenance and services**

Linking the virtual and real worlds along the entire value chain of customers

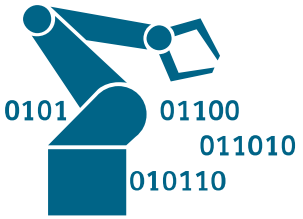
	Vertical software	Digital services
Revenue, FY 2015	€3.1 billion	€0.6 billion
Profitability	++	+++
Market growth	+9%	+15%

Concept for the Industrial Application of the Internet of Things – The Web of Systems provides security for critical infrastructure



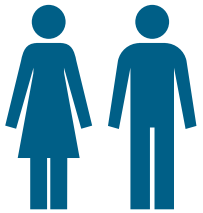
- Siemens believes the Internet of Things has tremendous potential
- In critical infrastructure, customers have much higher requirements regarding reliability, service life and data protection
- For this reason, in a Web of Systems the data is processed locally
- This ensures that the knowledge and the intellectual property of our customers remain protected
- Siemens is already using this technology in many projects today

Megatrends – Challenges that are transforming our world



Digitalization

By 2020, the digital universe will reach **44 zettabytes** – a tenfold increase from 2013.[1]



Demographic change

The earth's population will increase from 7.3 billion[2] people today to **9.7 billion**[2] in 2050. Average life expectancy will then be 83 years.[2]

Climate change

According to scientists, in the summer of 2016, the Earth's atmosphere had the **highest CO_2 concentration** in 800,000 years.[4]

Urbanization

By 2050, **70 percent of the world's population** will live in cities (today it's 54 percent).[3]

Globalization

The **volume of world trade** nearly **doubled** between **2005 and 2014.**[5]

Sources:

1. IDC, The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things, April 2014
2. United Nations, Department of Economic and Social Affairs, Population Division (2015). World Population Prospects: The 2015 Revision, Key Findings and Advance Tables. Working Paper No. ESA/P/WP.241
3. United Nations, World Urbanization Prospects. The 2014 Revision, New York, published 2015
4. SCRIPPS INSTITUTE OF OCEANOGRAPHY, "The Keeling Curve", July 30th, 2016
5. UNCTAD Statistics, Values and shares of merchandise exports and imports from 1948 to 2014, November 10, 2015

Concrete examples of our work – Core elements for the success of Digitalization

Intelligent industrial networking via Internet

We extended the concept of the Internet of Things for industrial applications: A digital networked world full of devices which are connected to the Internet has an influence how we control factories or critical infrastructures. Our Web of Systems makes these interactions reliable, safe, durable and can be used to "digitally toughen up“ existing plants.

Further information is available here: Pictures of the Future

Optimizing maintenance intervals

From trains to turbines, a vast range of machines generate and transmit data every second. With the technology platform Sinalytics we extract valuable information from this data to provide benefits for our customers. CT is responsible for this platform which brings together all of the technological components needed for data integration and analysis, connectivity, and cyber security.

Further information is available here: Pictures of the Future